AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An arrangement for protection of end user personal profile data in a communication system including ~~comprising~~ a number of end user stations and a number of service/information/content providers or holding means holding end user personal profile data, comprising:

~~characterized in~~

~~that it comprises~~ an intermediate proxy server supporting a first communication protocol for end user station communication; ~~and comprising~~

means for providing published certificates;~~,~~

a personal profile data protection server supporting a second communication protocol for communication with the intermediary proxy server and a third communication protocol for communication with one of said ~~a~~ service/information/content providers, said personal profile data protection server further comprises ~~and~~ an application programming interface (API) allowing service/information/content provider queries/interactions, and ~~comprising~~ storing means for storing of end user specific data and end user personal profile data;~~,~~ and

wherein ~~in that~~ the intermediary proxy server further comprises means for verifying the genuinity of a certificate requested over said second communication protocol from the personal profile protection server against a published certificate and in that the service/ information content server can request, via the API, personal profile data and in that personal profile data is delivered according to end user preferences or in such a manner that there is no association between the actual end user and the personal profile data of the end user.

2. (Currently Amended) An arrangement according to claim 1, wherein ~~characterized in that~~ the first communications protocol is a secure protocol.

3.-4. (Canceled)

5. (Currently Amended) An arrangement according to claim 1, wherein ~~any one of clams 1-3, characterized in that~~ the second protocol is a secure protocol~~, e.g. HTTP-S or IP Sec~~.

6. (Canceled)

7. (Currently Amended) An arrangement according to claim 1, wherein ~~any one of the preceding claims, characterized in that~~ the intermediary proxy server is a HTTP proxy.

8. (Currently Amended) An arrangement according to claim 1, wherein ~~any one of the preceding claims, characterized in that~~ the intermediary proxy server comprises holding means for holding published certificates.

9. (Currently Amended) An arrangement according to claim 1, wherein ~~any one of claims 1-7, characterized in that~~ the intermediary proxy server is in communication with external holding means holding published certificates.

10. (Canceled)

11. (Currently Amended) An arrangement according to claim 1, wherein ~~any one of claims 1-9, characterized in that~~ the intermediary proxy server is located within an intranet or at the operator's premises.

12. (Currently Amended) An arrangement according to claim 1, wherein ~~any one of the preceding claims, characterized in that~~ the intermediary proxy server

comprises a functionality for establishing a security communication agreement ~~(e.g. P3P or a natural language agreement)~~ with the protection server.

13. (Currently Amended) An arrangement according to claim 12, wherein ~~characterized in that~~ the user preferences are stored in the end user station.

14. (Currently Amended) An arrangement according to claim 12, wherein ~~characterized in that~~ the user preferences relating to privacy level are stored in the intermediary proxy server.

15. (Currently Amended) An arrangement according to claim 13, wherein ~~or 14, characterized in that~~ the user preferences relating to privacy level are stored in separate fast access storing means after completion of the security communication agreement.

16. (Currently Amended) An arrangement according to claim 15, wherein ~~any one of the preceding claims, characterized in that~~ the protection server comprises an API allowing service provider control of site and page policies, and in that if the end user privacy level is increased, data below the privacy level is deleted.

17. (Currently Amended) An arrangement according to claim 16, wherein ~~characterized in that~~ the protection proxy server provides certificates, and preferably signatures upon request by said intermediary proxy server.

18.-19. (Canceled)

20. (Currently Amended) An arrangement according to claim 1, wherein ~~19, characterized in that~~ the protection server storing means comprises at least three tables containing information about end user specific data, personal profile data information and statistical data respectively.

21. (Currently Amended) An arrangement according to claim 20, wherein the ~~19 or 20, characterized in that~~ end user specific data and end user personal profile data is provided to the service provider in such a manner that the end user cannot be traced by the service provider. ~~, i.e. without end user association.~~

22. (Currently Amended) An arrangement according to claim 21, wherein ~~characterized in that~~ the protection proxy server comprises means for pseudonymizing statistical information and personal profile information by using a unique pseudo for each URL of the service provider that is requested.

23. (Currently Amended) A method for protection of end user personal profile data in a communication system with a number of end user stations and a number of service/information/content providers, comprising the steps of:

~~characterized in~~

~~that it comprises the steps of:~~

- registering a certificate for an end user personal profile protection server with a trusted third party;
- providing a request for the certificate ~~(and signed content)~~ from an intermediary proxy server in communication with an end user station using a first communication protocol, to the protection server over a second communication protocol,
- providing a response from the protection server to the intermediary server,
- verifying, in the intermediary proxy server that the certificate is genuine, thereby belonging ~~i.e. belongs~~ to the respective protection server and is registered with the trusted third party,
- after confirmation that the protection server/ certificate is genuine,
- allowing the service provider having acquired the protection server to retrieve end user data and personal profile data according to policy setting and end user privacy level over an Application Programming Interface and a third communication protocol.

24. (Currently Amended) The method according to claim 23, further comprising the step of ~~characterized in that it further comprises the step of:~~ establishing an end user personal profile data security agreement between the intermediary proxy server and the protection server (on behalf of the end user and the service provider).

25. (Currently Amended) The method according to claim 24, wherein ~~characterized in that~~ the agreement comprises a P3P agreement.

26.-28. (Canceled)

29. (Currently Amended) The method according to claim 23, wherein ~~any one of claims 23-28, characterized in that~~ the end user preferences (privacy levels) are stored in the end user station or in the intermediary proxy server, and in that they can be separately stored after confirmation of the agreement.

30. (Currently Amended) The method according to claim 23, further comprising the steps of: ~~any one of claims 23-29, characterized in that it comprises the steps of:~~

- providing an API at the protection server,
- using the API for queries to the protection servers from the service provider,
- providing responses over a third communication protocol to the service provider.

31. (Currently Amended) The method of claim 30, further comprising the step of ~~characterized in that it comprises the steps of:~~ storing data in a number of tables in the protection server relating to user specific data, end user personal profile data and statistical data.

32. (Currently Amended) The method of claim 31, further comprising the step of ~~characterized in that it comprises the step of:~~ pseudonymizing statistical data and profile information such that end user personal data cannot be associated or tied to the actual end user.